IJNRD.ORG ISSN : 2456-4184
INTERNATIONAL JOURNAL OF NOVEL RESEARCH AND DEVELOPMENT (IJNRD) | IJNRD.ORG
An International Open Access, Peer-reviewed, Refereed Journal

Secure EHR Management Using CP-ABE and Smart Contract-Based Blockchain Systems

[1]PALLA GANGAMMA,
Student in Dept. Of Master of Computer Applications, at Miracle Educational Society Group of Institutions
[2]U SIRISHA, Miracle Educational Society Group of Institutions
[3]Dr. LEKKALA CHINNNARI, Miracle Educational Society Group of Institutions
[1]sravanijaggu699@gmail.com

ABSTRACT:

This project combines Attribute-Based Encryption (ABE) and Blockchain technology for the first time for the purpose of securing and preserving the integrity of Electronic Health Records (EHRs). It introduces the CEC-ABE algorithm, which is an enhanced version of CP-ABE, which supports the decentralization of the decryption process while constraining access based on user attributes. Smart contracts enabled on the Ethereum blockchain provide guarantees for data immutability and traceability which enforces that only authorized users interact with the sensitive health data. In addition, some machine learning models like Random Forest and SVM are applied for reliable and accurate medical diagnosis. The system is implemented on a Django web framework which provides an interactive interface in real time and improves the security of data for the users, data providers, and patients.

Keywords: ABE, Smart Contracts, EHRs

INTRODUCTION

In the health care systems today, protecting and preserving the integrity of Electronic Health Records (EHRs) is an ever-present challenge. Security risks, unauthorized access, and breaches of privacy are some of the problems that occur on systems that are cloud-based and database-centric because the databases are stored in a single location, and the access control is minimal. This document is intended to demonstrate the application of CP-ABE in the blockchain technology setting to address the de-centralization, security, and privacy of the Electronic Health Records system. The CEC-ABE algorithm as proposed supports fine-grained access control where only users with specific attributes can decrypt sensitive information. The Ethereum blockchain guarantees immutability, auditability, and protection against tampering. Furthermore, integrating machine learning algorithms such as Random Forest and SVM aids the system in identifying diseases at an early stage and improving clinical workflows. Through Django, an interface has been

developed which enables interaction among patients and doctors and supports the secure creation, confirmation, and management of EHRs and prescriptions.

RELATED WORK

Wang et al. (2017) proposed an Identity-Based Data Outsourcing (IBDO) model which enables secure proxy uploads while providing advanced auditing capabilities regarding the file's integrity and origin. This model was a precursor for enabling data traceability in cloud-based storage systems. Zhang & Xu (2019) proposed HealthDep, a document deduplication procedure for electronic medical records in eHealth systems. It drastically decreased the storage overhead while upholding data confidentiality, thus providing an efficient solution for large-scale data storage. Bethencourt & Sahai (2007) were the first to CP-ABE and support sophisticated access control policies embedded directly to the ciphertext. Their scheme has collusion resistance and is appropriate for untrusted clouds. Wang et al. (2021) designed a mobile healthcare network-centric lightweight CP-ABE framework. This method utilizes Boneh–Lynn–Shacham signatures to verify computations which are offloaded to semi-trusted devices, therefore, making it suitable for low-power devices. HealthChain, introduced by Xu et al. (2022), is a blockchain-based system that preserves privacy while ensuring the integrity and immutability of health data, allowing for key revocation and fine-grained access.

TABLE1. Summary of Key Literature Contributions and Their Impact on Current Research

Author	Contribution	Impact on Research
Wang et al.	Identity-based data outsourcing with proxy auditing	Introduced auditing of origin and user-specific upload control
Zhang & Xu	HealthDep deduplication in eHealth	Reduced EMR storage overhead while maintaining encryption
Bethencourt & Sahai	CP-ABE for flexible access control	Enabled encryption with user-specific attribute policies, improving cloud security
Wang et al.	Lightweight CP-ABE for mobile healthcare	Minimized computation on mobile devices while maintaining security
Xu et al.	Blockchain-based HealthChain for smart healthcare	Ensured data traceability and immutable storage with blockchain

PROPOSED APPROACH

The system intends to enhance the security of Electronic Health Records (EHRs) by implementing a hybrid framework which incorporates Ciphertext-Policy Attribute-Based Encryption (CP-ABE), blockchain, and machine learning. To achieve this, a

new encryption method, CEC-ABE, is introduced to allow greater decentralization of the decryption process while applying strict access controls based on user attributes. The data is encrypted using CE-ABE and the encryption is stored on an Ethereum blockchain, which is tamper-proof, through smart contracts developed in Solidity. This way, only properly attributed and validated users can access the data, thus preserving the privacy and integrity of the patient. The system incorporates machine learning models such as Random Forest and SVM to predict heart conditions based on user inputs, aiding doctors in providing precise and timely diagnostic estimates. The Django-based web application offers an intuitive interface for managing EHRs, enabling users to register, log in, write prescriptions, and confirm EHRs. This approach provides a comprehensive solution for a secure, decentralized, and intelligent healthcare data management system, giving full control, traceability, and cognitive assistive diagnostics to the patients and healthcare practitioners.

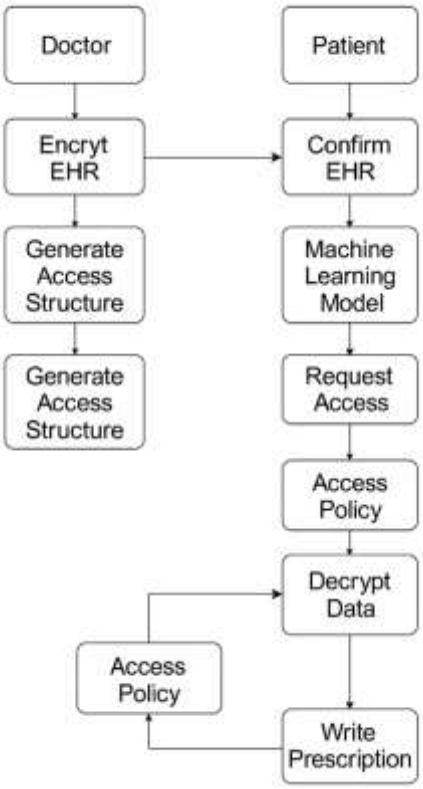


Figure 1: Proposed EHR management System

METHODOLOGIES

Frontend and Backend Design: A Django-based web application provides interfaces for doctors and patients to interact with EHRs. Functionalities include user registration, login, EHR creation, confirmation, and prescription entry.

Attribute-Based Encryption (CEC-ABE): The CE-ABE algorithm encrypts sensitive data using access control policies. Users can only decrypt data if their attributes match the defined access policy. Key generation, encryption, and decryption processes are implemented using elliptic curve cryptography (ECIES).

Blockchain Integration: Ethereum blockchain is integrated using Web3.py.

Smart contracts written in Solidity are deployed to manage immutable storage of EHRs and prescriptions. Functions such as createEHR and updateStatus ensure secure transaction logging and access tracking.

Machine Learning Models: Historical medical data is preprocessed and used to train Random Forest and SVM models for heart disease prediction. These models are integrated into the Django app to provide real-time analysis during EHR creation.

Security and Access Control: User authentication is handled using Django's session management. CE-ABE ensures that only authorized users can view or modify data. Blockchain adds an additional immutable audit trail.

Data Flow: When a doctor creates an EHR, the data is encrypted using CE-ABE, stored on the blockchain, and then verified and confirmed by the patient. Follow-up doctors access the data through smart contract calls and contribute additional prescriptions.

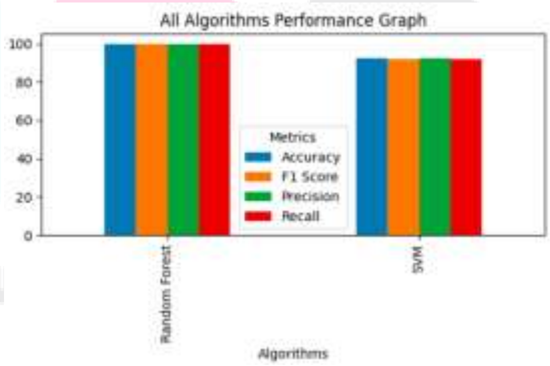
RESULTS

The system was successfully developed and tested in a simulated environment using Django, Ethereum blockchain, and real-world medical datasets. Two machine learning models Random Forest and SVM were trained to predict heart disease from clinical data. The Random Forest classifier achieved higher accuracy compared to SVM, confirming its suitability for medical diagnostics.

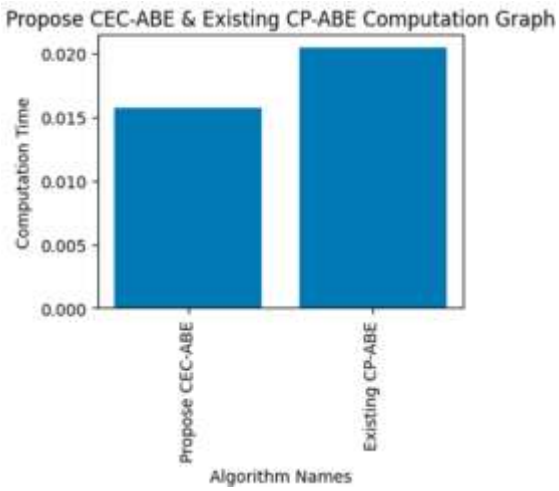
The proposed CEC-ABE algorithm was benchmarked against standard CP-ABE. Results showed that CEC-ABE significantly reduced decryption computation time by decentralizing the process. Additionally, the use of blockchain ensured that EHRs remained immutable and transparent, with verifiable transaction records.

During EHR creation, encrypted data and machine learning-based predictions were securely stored on-chain. Decryption was possible only when user attributes matched the policy, ensuring fine-grained access control. A graphical representation compared computation times between CEC-ABE and CP-ABE, clearly demonstrating the efficiency of the proposed system.

Algorithm Name	Accuracy	Precision	Recall	FSCORE
Random Forest	100.0	100.0	100.0	100.0
SVM	92.10526315789472	92.17673436557143	92.09652179843044	92.05734231545944



Random Forest and SVM training completed and their performance, Graph



Graph x-axis represents algorithm names and y-axis represents computation time and in both algorithms propose got less time

DISCUSSION

The integration of Attribute-Based Encryption (ABE) with blockchain addresses several core challenges in EHR management, notably data privacy, unauthorized access, and trustless validation. Unlike traditional centralized healthcare systems, this project leverages CP-ABE's attribute-based access control and blockchain's immutability to create a decentralized and transparent ecosystem.

By introducing the CEC-ABE model, the system reduces computational bottlenecks typically associated with CP-ABE, making it suitable for real-time healthcare environments. Additionally, the use of smart contracts enforces data policies at a structural level, removing the need for intermediaries and reducing reliance on central authorities.

The system also enhances medical decision-making through the integration of machine learning. Random Forest and SVM models offer diagnostic support, making the system not just secure but also intelligent.

CONCLUSION

This work illustrates the secure and intelligent framework for managing Electronic Health Records (EHRs) based on blockchain technology and attribute-based encryption. It provides a novel approach with the CEC-ABE model which guarantees efficient and decentralized decryption while allowing fine-grained access control. Integrating blockchain guarantees data integrity, transparency, and auditability. Smart contracts provide the means to enable non-reputable and permanent record-keeping while machine learning aids in improving the accuracy of the diagnosis. The interface based on Django guarantees usability for patients and healthcare providers, allowing EHRs to be created and confirmed and prescriptions to be managed. The experiments performed within this model also confirm its improved performance over CP-ABE in access control and computation time. As a whole, the systems provide a scalable, privacy preserving framework designed for modern health care systems with unrestricted complexity.

REFERENCES

[1] X. Li, L. Jin, and H. Kan, ‘‘Air pollution: A global problem needs local

fixes,'' Nature, vol. 570, no. 7762, pp. 437–439, Jun. 2019.

[2] Y. Han, J. C. K. Lam, and V. O. K. Li, ''A Bayesian LSTM model to evaluate the effects of air pollution control regulations in China,'' in Proc. IEEE Big Data Workshop (Big Data), Dec. 2018, pp. 4465–4468.

[3] L. Bai, J. Wang, X. Ma, and H. Lu, ''Air pollution forecasts: An overview,'' Int. J. Environ. Res. Public Health, vol. 15, no. 4, p. 780, 2018.

[4] Y. Ding and Y. Xue, ''A deep learning approach to writer identification using inertial sensor data of air-handwriting,'' IEICE Trans. Inf. Syst., vol. E102-D, no. 10, pp. 2059–2063, 2019.

[5] S.-Q. Dotse, M. I. Petra, L. Dagar, and L. C. De Silva, ''Application of computational intelligence techniques to forecast daily PM10 exceedances in Brunei Darussalam,'' Atmos. Pollut. Res., vol. 9, no. 2, pp. 358–368, Mar. 2018.

[6] M. Jia, A. Komeily, Y. Wang, and R. S. Srinivasan, ''Adopting Internet of Things for the development of smart buildings: A review of enabling technologies and applications,'' Automat. Construct., vol. 101, pp. 111–126, May 2019.

[7] S. Abirami, P. Chitra, R. Madhumitha, and S. R. Kesavan, ''Hybrid spatio-temporal deep learning framework for particulate matter (PM2.5) concentration forecasting,'' in Proc. Int. Conf. Innov. Trends Inf. Technol. (ICITIIT), Feb. 2020, pp. 1–6.

[8] Y. Cheng, S. Zhang, C. Huan, M. O. Oladokun, and Z. Lin, ''Optimization on fresh outdoor air ratio of air conditioning system with stratum ventilation for both targeted indoor air quality and maximal energy saving,'' Building Environ., vol. 147, pp. 11–22, Jan. 2019.

[9] A. C. Cosma and R. Simha, ''Machine learning method for real-time non-invasive prediction of individual thermal preference in transient conditions,'' Building Environ., vol. 148, pp. 372–383, Jan. 2019.

[10] M. Bhowmik, K. Deb, A. Debnath, and B. Saha, ''Mixed phase Fe2O3/Mn3O4 magnetic nanocomposite for enhanced adsorption of methyl orange dye: Neural network modeling and response surface methodology optimization,'' Appl. Organometallic Chem., vol. 32, no. 3, p. e4186, Mar. 2018.

[11] V. Chaudhary, A. Deshbhratar, V. Kumar, and D. Paul, ''Time series based LSTM model to predict air pollutant's concentration for prominent cities in India,'' in Proc. Int. Workshop Utility-Driven Mining (UDM), Aug. 2018, pp. 1–9.

[12] M. Chen, J. Yang, L. Hu, M. S. Hossain, and G. Muhammad, ''Urban healthcare big data system based on crowdsourced and cloud-based air quality indicators,'' IEEE Commun. Mag., vol. 56, no. 11, pp. 14–20, Nov. 2018.

[13] R. Chen, X. Wang, W. Zhang, X. Zhu, A. Li, and C. Yang, ‘‘A hybrid CNN-LSTM model for typhoon formation forecasting,’’ GeoInformatica, vol. 23, no. 3, pp. 375–396, Jul. 2019.

[14] S. Du, T. Li, Y. Yang, and S. Horng, ‘‘Deep air quality forecasting using hybrid deep learning framework,’’ IEEE Trans. Knowl. Data Eng., vol. 33, no. 6, pp. 2412–2424, Jun. 2021.

[15] R. Feng, H.-J. Zheng, H. Gao, A.-R. Zhang, C. Huang, J.-X. Zhang, K. Luo, and J.-R. Fan, ‘‘Recurrent neural network and random forest for analysis and accurate forecast of atmospheric pollutants: A case study in Hangzhou, China,’’ J. Cleaner Prod., vol. 231, pp. 1005–1015, Sep. 2019.

[16] B. S. Freeman, G. Taylor, B. Gharabaghi, and J. Thé, ‘‘Forecasting air quality time series using deep learning,’’ J. Air Waste Manage. Assoc., vol. 68, no. 8, pp. 866–886, Aug. 2018.

[17] S. Mahajan, H.-M. Liu, T.-C. Tsai, and L.-J. Chen, ‘‘Improving the accuracy and efficiency of PM2.5 forecast service using cluster-based hybrid neural network model,’’ IEEE Access, vol. 6, pp. 19193–19204, 2018.

[18] J. Jin, J. Gubbi, S. Marusic, and M. Palaniswami, ‘‘An information framework for creating a smart city through Internet of Things,’’ IEEE Internet Things J., vol. 1, no. 2, pp. 112–121, Apr. 2014.

[19] A. Grover, A. Kapoor, and E. Horvitz, ‘‘A deep hybrid model for weather forecasting,’’ in Proc. 21st ACM SIGKDD Int. Conf. Knowl. DiscoveryData Mining, Aug. 2015, p. 379–386.

[20] A. Agarwal and M. Sahu, ‘‘Forecasting PM2.5 concentrations using statistical modeling for Bengaluru and Delhi regions,’’ Environ. Monit. Assessment, vol. 195, p. 502, Mar. 2023.